Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	Your organization, a multimedia company that provides marketing and design services to small businesses, experienced a DDoS attack. The internal network was disrupted for two hours due to a flood of ICMP packets sent through an unconfigured firewall. The attacker exploited this weakness to overwhelm the network, making internal resources unavailable until the issue was resolved.
Identify	- The firewall did not have rules in place to limit ICMP traffic. - IDS/IPS systems were not configured to handle or detect large volumes of incoming ICMP packets. - Network monitoring tools were missing or not configured to detect abnormal traffic behavior. - The firewall lacked source IP address verification to filter out spoofed packets.
Protect	protect the asset of the company by: - enable rules limit for ICMP traffic on firewall. - enable verification source IP address filter for legitimate packets.

	- .
Detect	- configured IDS/IPS systems to handle and detect large columns of incoming ICMP packets. - configure network monitoring tools to detect abnormal traffic behaviors
Respond	- Blocked incoming ICMP packets to stop the DDoS traffic during the attack. - Disabled non-essential services to reduce network load and prioritize recovery. - Investigated firewall misconfigurations and updated rules to prevent further flooding. - Documented response steps and informed stakeholders of the ongoing situation.
Recover	- Re-enabled incoming ICMP traffic after confirming the threat was neutralized. - Restored non-essential services that were previously disabled during the response phase. - Returned to normal business operations within four hours of the incident resolution. - Conducted a recovery debrief and updated documentation to reflect lessons learned.

Reflections/Notes:

This was a quick and effective response to a serious security event. The IT team acted swiftly to eliminate the ICMP flooding issue by blocking all incoming ICMP traffic and temporarily shutting down non-critical services. They also implemented new firewall rules to prevent further flooding. Moving forward, the setup of IDS/IPS systems and network monitoring tools will help detect abnormal traffic patterns and automatically block suspicious activity, strengthening the organization's overall network security.